بسم الله الرحمن الرحيم

والسلام عليكم ورحمة الله وبركاته

الحمد لله ،والشكر له على توفيقه العام؛ وأشهد ألا إله إلا الله وحده لا شريك له؛وأشهد أن محمدا عبده ورسوله؛صلى الله عليه وعلى آله وصحبه هداة الأنام ومصابيح الظلام

أما بعد..

اليوم وبفضل الله سنشرح لكم طريقة حماية الجهاز من الفيروسات

وحذف فيروس أتوران وإظهار جميع الملفات المخفية بدون برنامج

من إعداد أخوكم في الله :

عثماني علاء الدين

من الجزائر

كتاب : الحماية بواسطة النظام

ولمزيد من المعلومات أو الأسئلة راسلوني عبر البريد التالي :

cheriaala@yahoo.com

فلا تنسونا من دعوة صالحة لي وللوالدين ولجميع المسلمين جزاكم الله خيرا

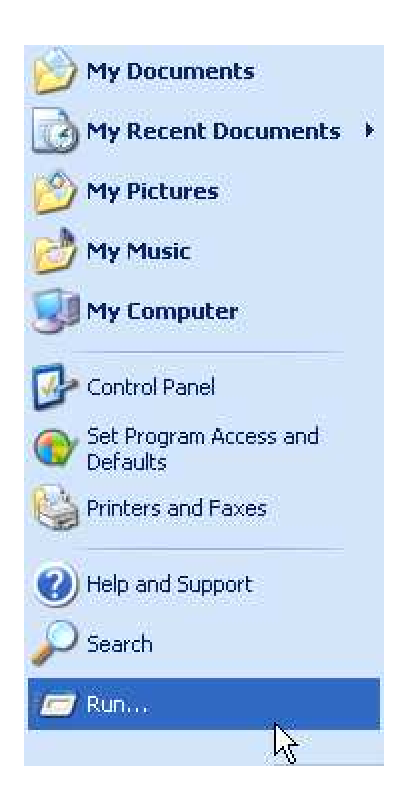
ولتطبيق هذه الطريقة نتبع المراحل التالي :

أخوكم في الله : عثماني علاء الدين

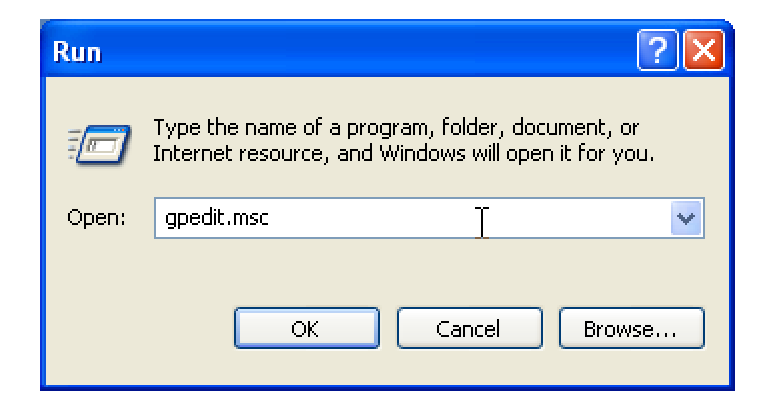
إعداد : عثماني علاء الدين **الجزائر**

أولا يجب أن نقوم بعمل مهم جدا وهو عمل متمثل في منع القراءة التلقائية للأقراص بكل أنواعها كي لا يستطيع الفيروس تشغيل نفسه عند إدخال إي قرص أو فلاش ديسك وهي كالتالي :

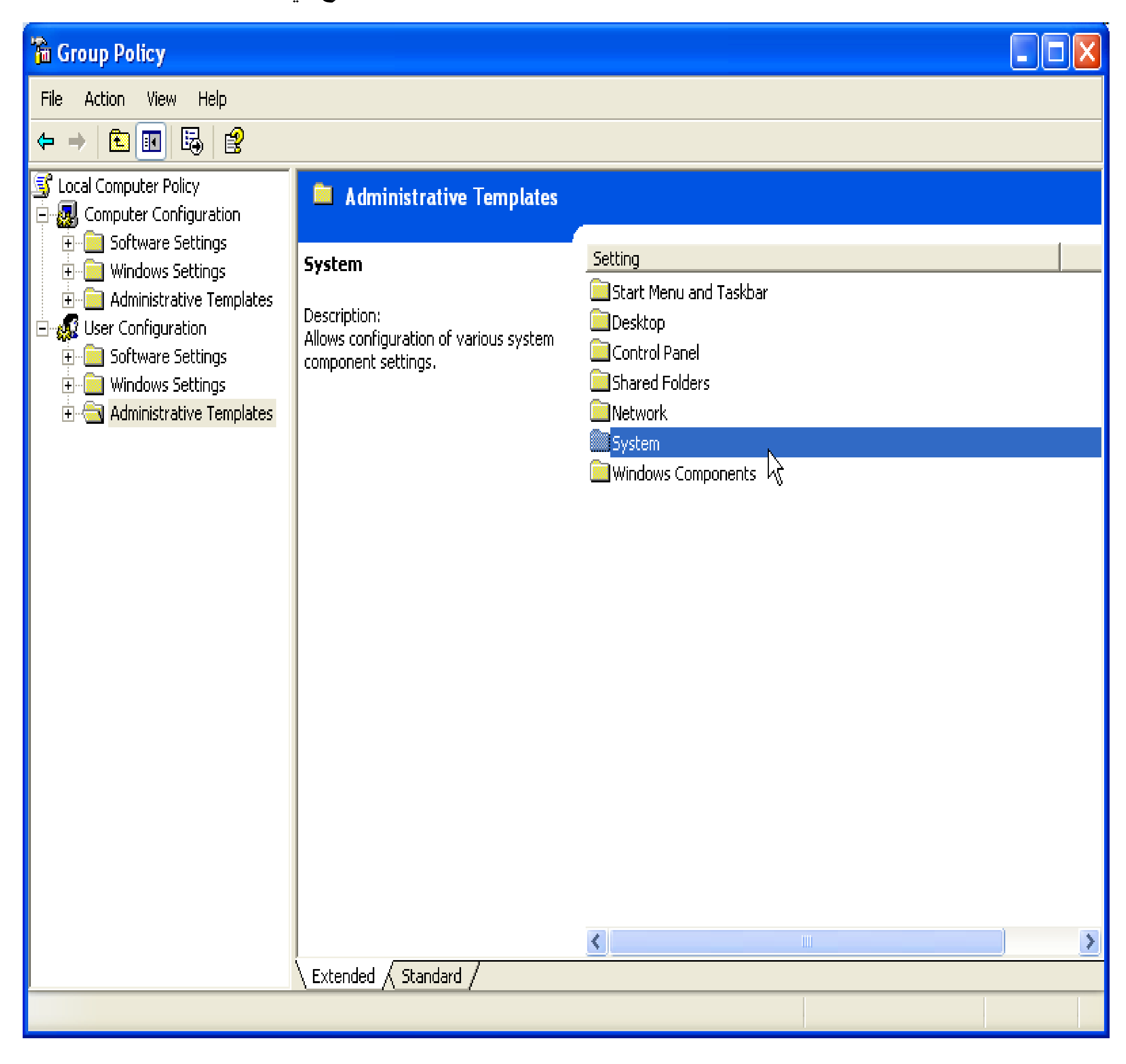
بعد النقر على زر أبدء نختار تشغيل كما هو موضح في الصورة



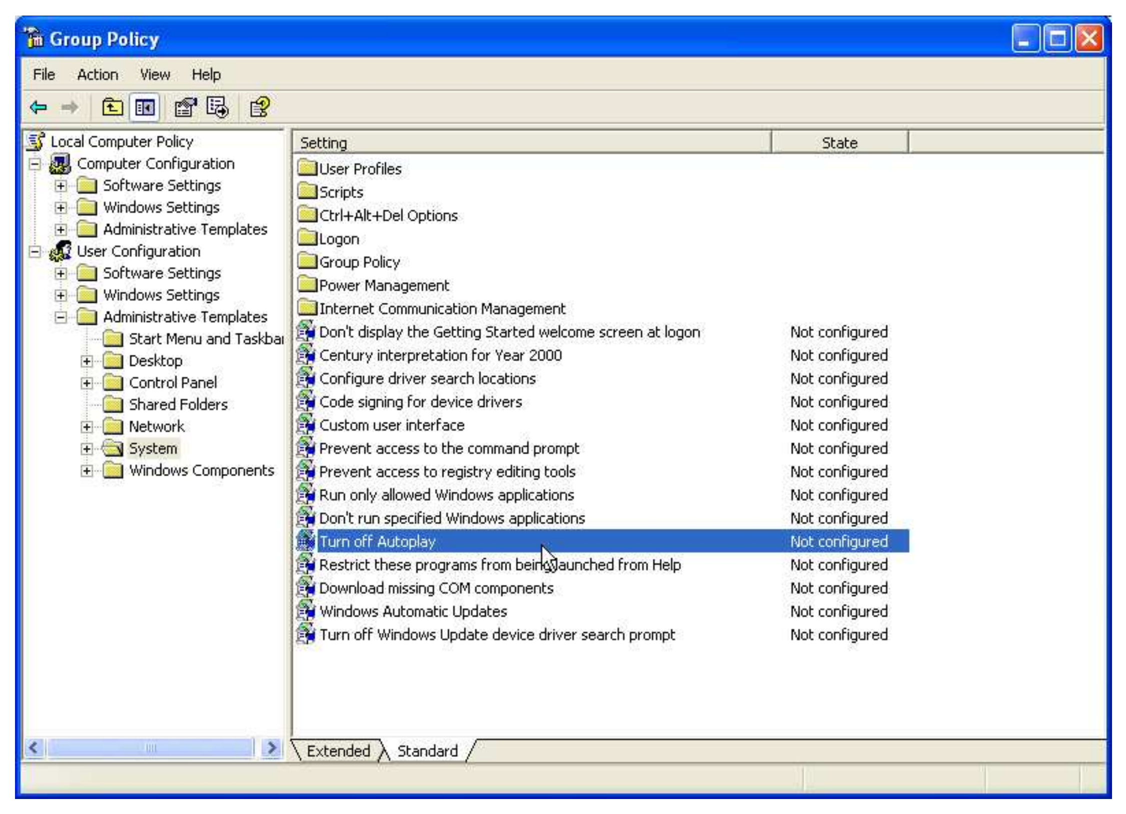
ثم ندخل التعليمة التالية gpedit.msc ثم نختار موافق



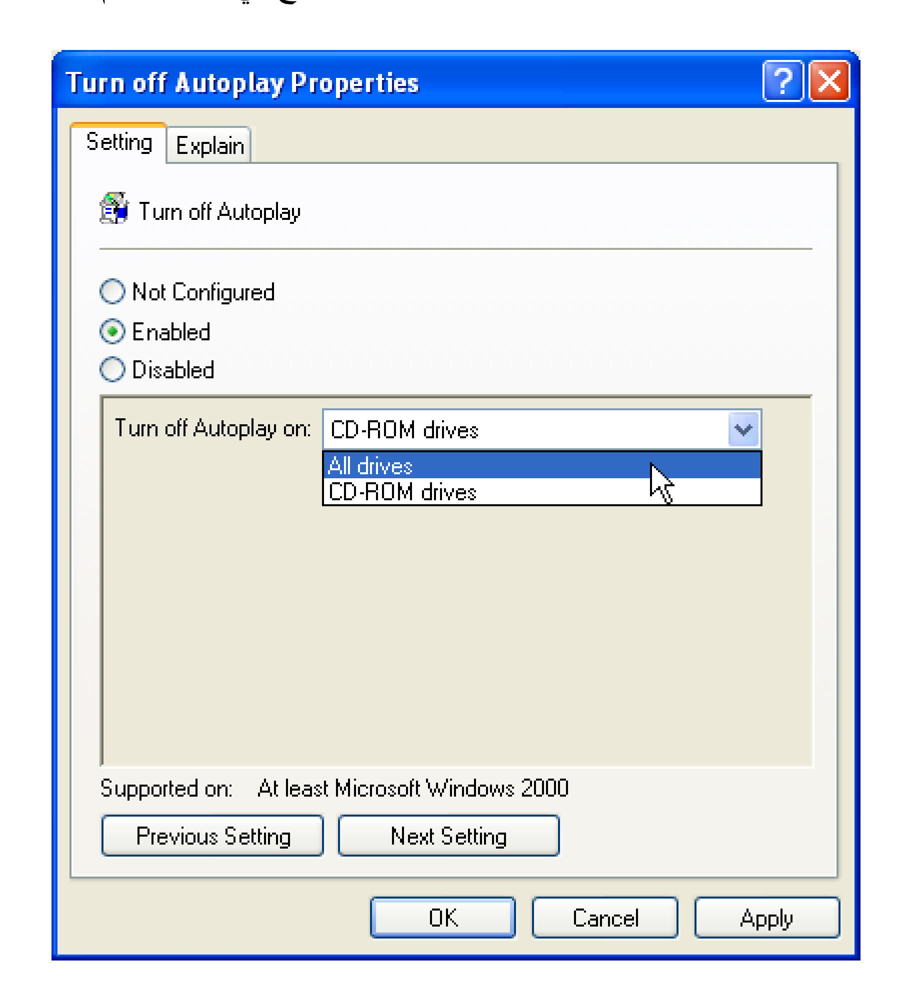
بعد ذلك تظهر لنا مجموعة من الخيارات نختار منها كما موضح في الصورة



بعد النقر على system تظهر مجموعة من الأسطر نختار كما موضح في الصورة

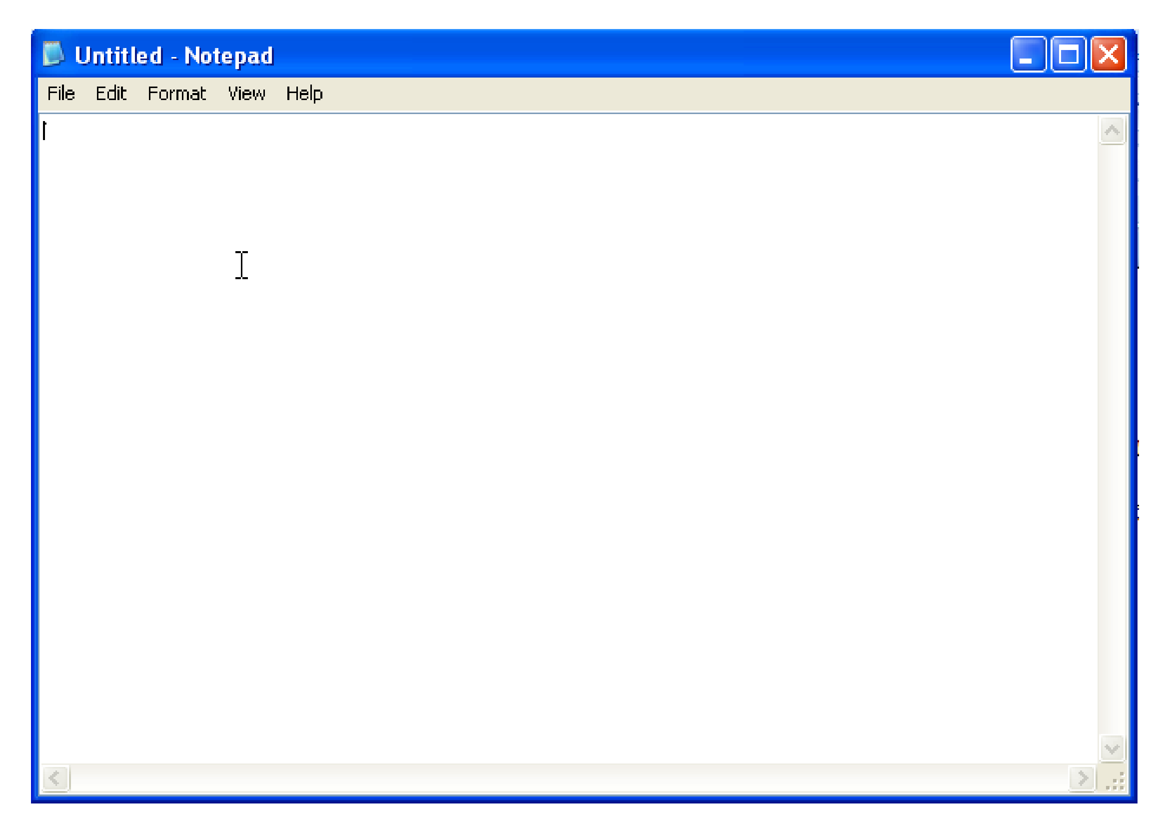


بعد النقر على هذا السطر تظهر لنا علبة حوار نختار منها كما موضح في الصورة ثم الضغط على موافق



وبعد إتمام هذه العملية

قم بفتح المفكرة :



ندخل فيه المعلومات التالية التي سيتم شرحها بإذن الله في الأخير

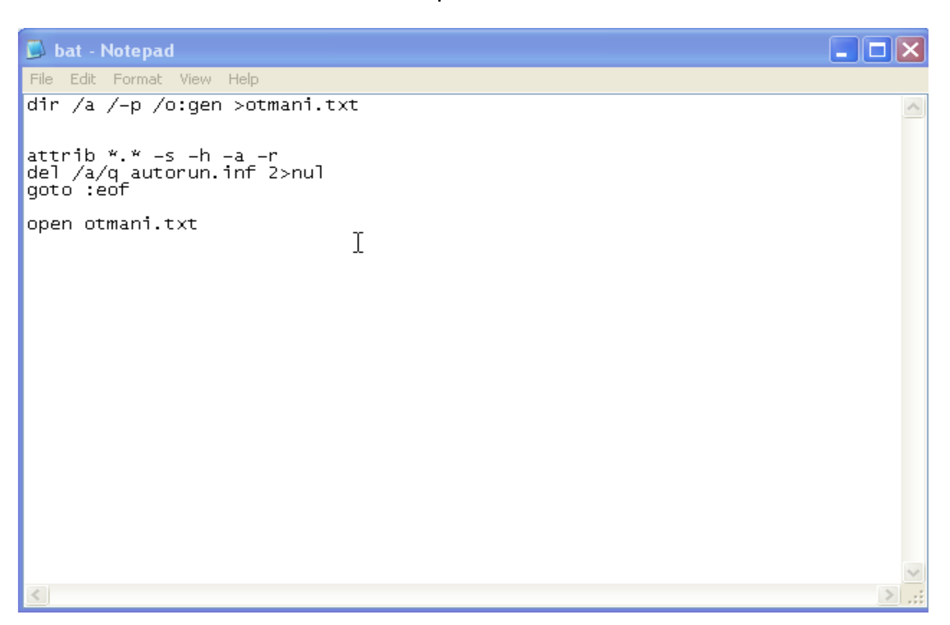
dir /a /-p /o:gen >otmani.txt

attrib *.* -s -h -a -r

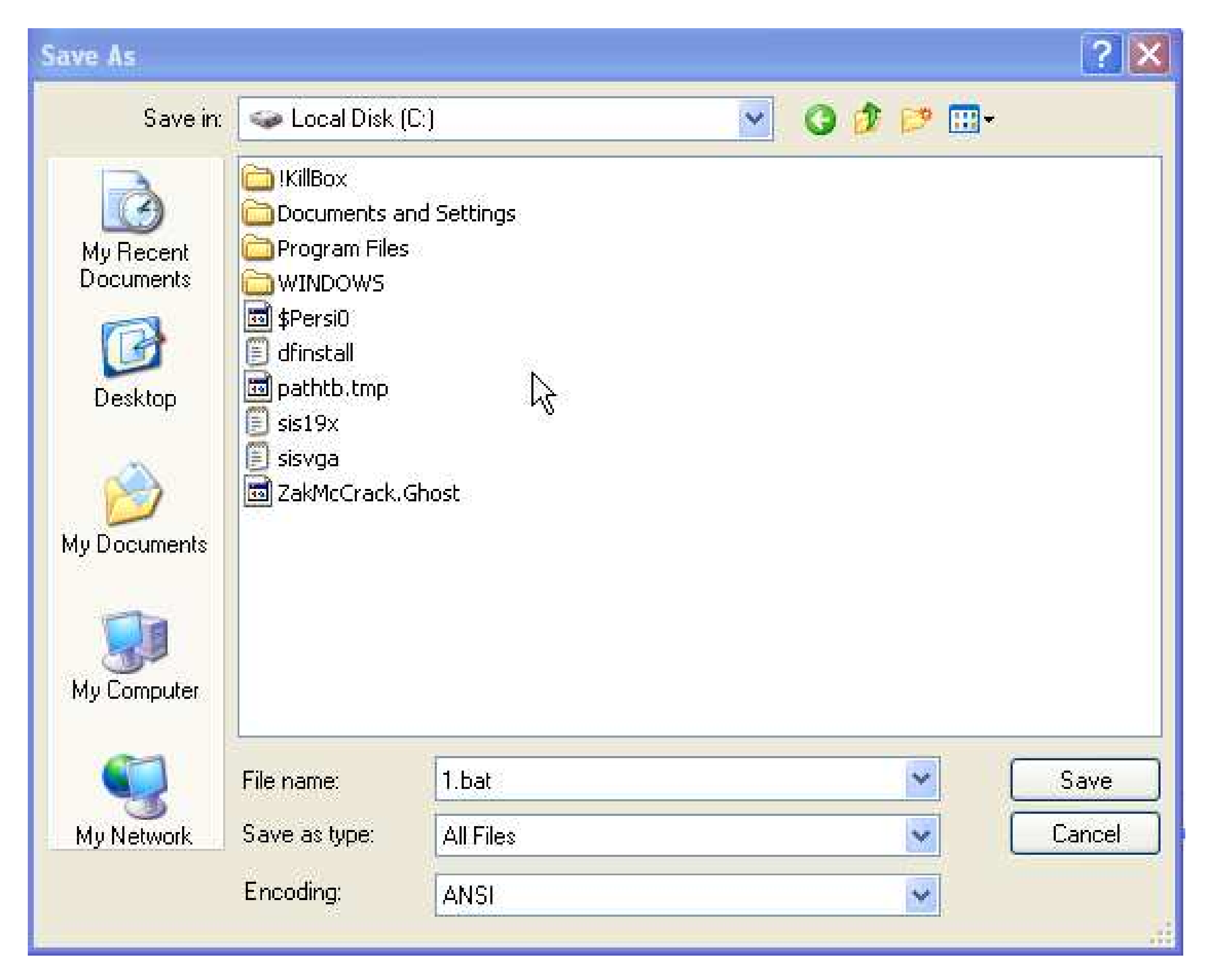
del /a/q autorun.inf 2>nul

goto :eof

open otmani.txt



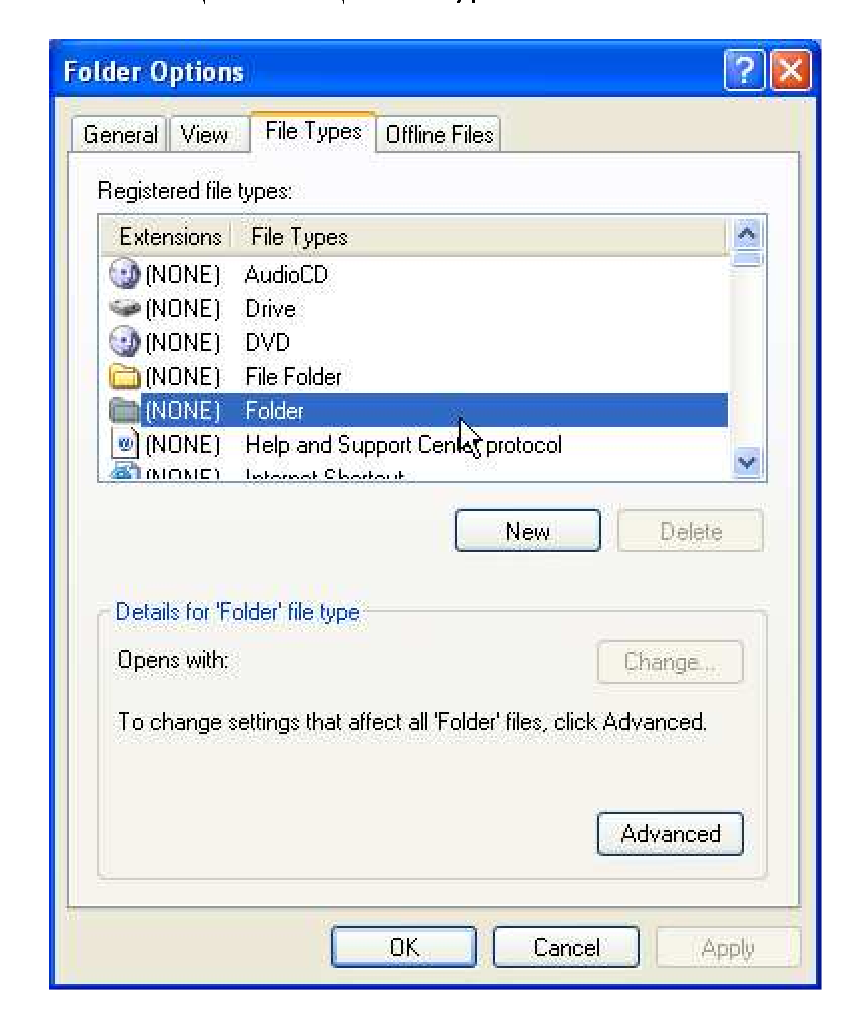
ثم نقوم بحفظ الملف في أي قرص وليكن القرص * C * بصيغة * bat * وإسمه مثلا : 1 بعد إختيار كافة الملفات من علبة الحوار



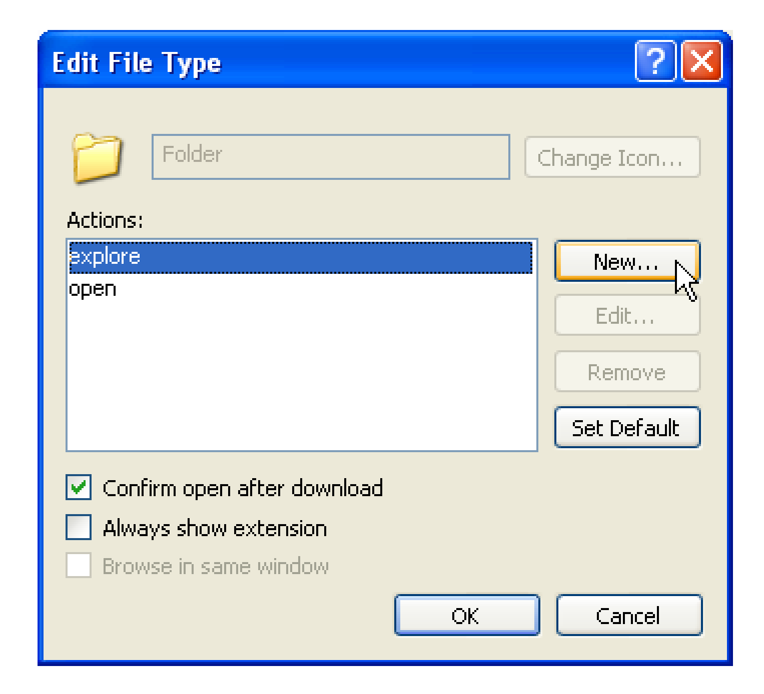
ثم نذهب إلى خيارات المجلد الموجودة في شريط القوائم لجهاز الكمبيوتر

My Computer
File Edit View Favorites Tools Help
Map Network Drive...
Disconnect Network Drive...
Synchronize...
Folder Options...
Back
Address My Computer
Go
System Tasks
View system information
Change a setting
Other Places
My Network Places
My Documents
Shared Documents
Control Panel
Details
Shared Documents
ala-eddine's Documents
otmani's Documents
Hard Disk Drives
Local Disk (C:)
D (D:)
E (E:)

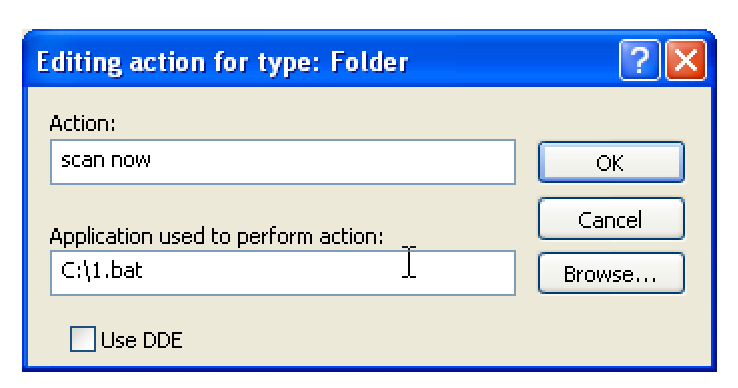
وبعد ذلك نختار من علبة الحوار File Types ثم Folder ثم نختار Advanced



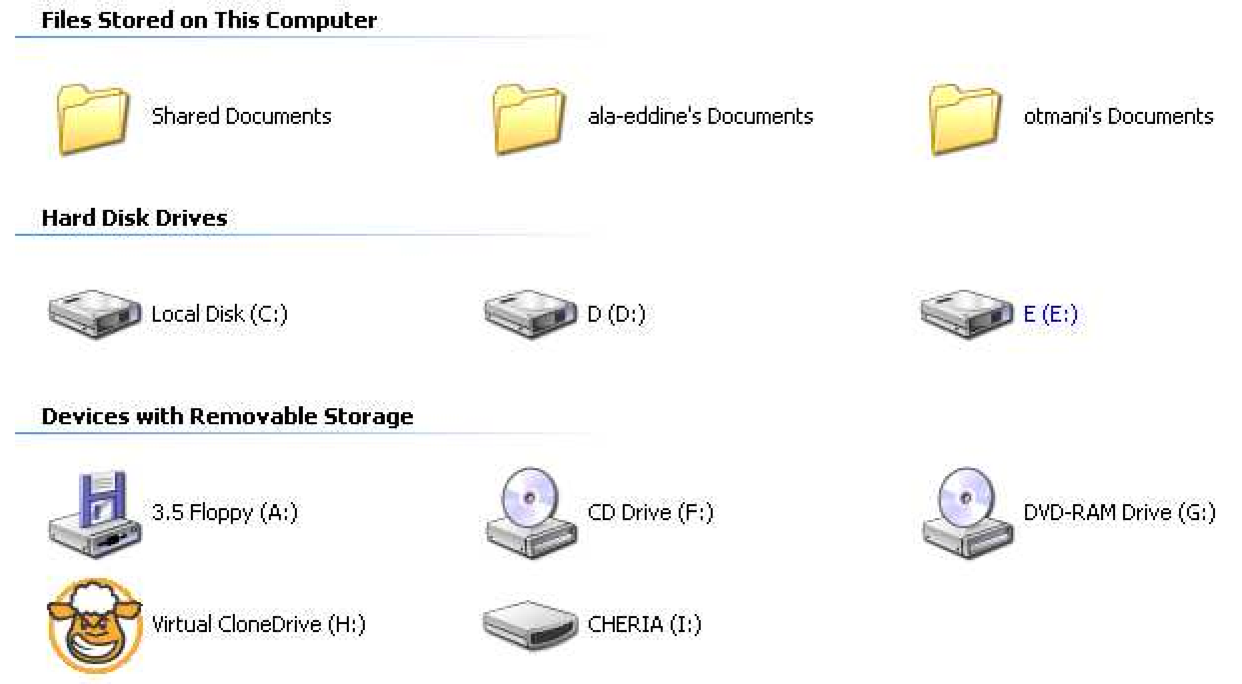
ثم نختار New



وندخل الاسم الذي نريده ولكين scan now وفي المكان الثاني نحدد مسار الملف الذي عملناه ثم نختار موافق



ونبدأ الآن بتطبيق ذلك على جهاز فلاش ديسك



My Computer
File Edit View Favorites Tools Help
Back Search Folders
Address My Computer Go

System Tasks
View system information
Change a setting
Eject this disk

Other Places
My Network Places
My Documents
Shared Documents
Control Panel

Details
CHERIA (I:)
Removable Disk
File System: FAT32

Files Stored on This Computer
Shared Documents ala-e ani's Documents
Hard Disk Drives
Local Disk (C:) D (D :)
Devices with Removable Storage
3.5 Floppy (A:) CD D -RAM Drive (G:)
Virtual CloneDrive (H:) CHE

Open
AutoPlay
Explore
Search...
scan now
Sharing and Security...
Save to Solid Capture
Add to archive...
Add to "Archive.rar"
Compress and email...
Compress to "Archive.rar" and email
Format...
Eject
Cut
Copy
Create Shortcut
Rename
Properties

بعد القيام بعملية نختار Folders أو استكشاف كما في الصورة

My Computer
File Edit View Favorites Tools Help
Back Search Folders
Address My Computer Go

System Tasks
View system information
Change a setting

Other Places
My Network Places
My Documents
Shared Documents
Control Panel

Details
My Computer
System Folder

Files Stored on This Computer
Shared Documents
ala-eddine's Documents
otmani's Documents

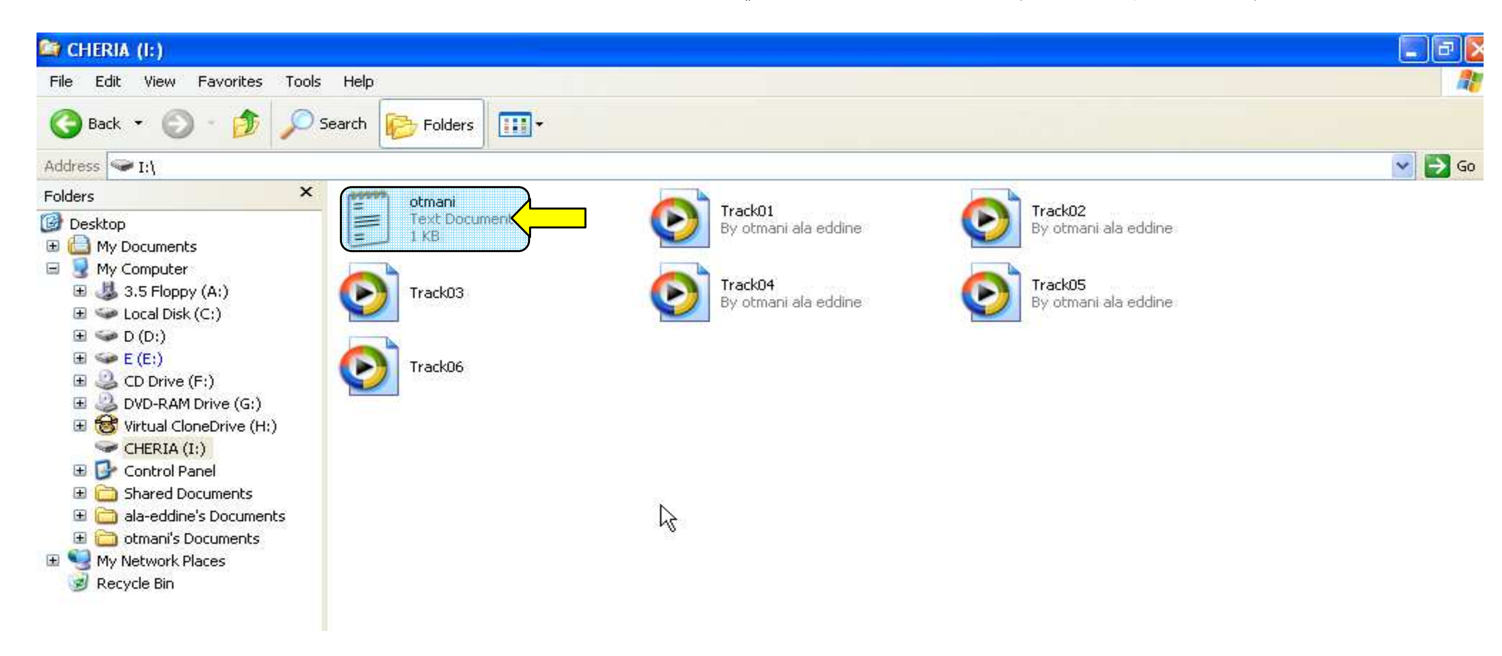
Hard Disk Drives
Local Disk (C:)
D (D:)
E (E:)

Devices with Removable Storage
3.5 Floppy (A:)
CD Drive (F:)
DVD-RAM Drive (G:)
Virtual CloneDrive (H:)
CHERIA (I:)

ثم نختار جهاز فلاش ديسك ستعرض لنا الملفات الموضحة في الصورة



والأن للننظر الملف الذي أمرنا النظام بإنشائه الذي على شكل نص وهو مبين في الصورة



وعندما نفته نجد التالي :

otmani - Notepad

File Edit Format View Help

```
 Volume in drive I is CHERIA
 Volume Serial Number is 1CF7-5906

 Directory of I:\

11/13/2008  11:47 AM           262,595 xpbkh.com
11/21/2008  07:36 PM           154,781 zPharaoh.exe
11/21/2008  07:38 PM               126 autorun.inf
11/20/2008  10:13 PM         5,427,343 Track01.mp3
11/20/2008  10:13 PM         5,680,209 Track02.mp3
11/20/2008  10:13 PM         4,953,795 Track03.mp3
11/20/2008  10:13 PM         3,148,050 Track04.mp3
12/07/2008  07:31 PM         6,798,923 Track05.mp3
11/20/2008  10:13 PM         5,211,258 Track06.mp3
12/15/2008  04:54 PM                 0 otmani.txt
              10 File(s)     31,637,080 bytes
               0 Dir(s)     975,044,608 bytes free
```

هذه الفيروسات التي كانت في الفلاش ديسك وبفضل الله تم حذف مشغل الفيروس تلقائيا وهو الملف مسمى autorun.inf ثم يتم إظهار جميع الملفات الموجودة ستظهر لنا مجموعة من الملفات المشبوهة بها فنقوم بحذفها

شرح الأوامر المطبقة

dir /a /-p /o:gen >otmani.txt

هذا الأمر لإعطاء نظرة على الملفات الموجودة قبل التعديل علبها

attrib *.* -s -h -a –r

هذا الأمر لإظهار جميع الملفات المخفية

del /a/q autorun.inf 2>nul

هذا الأمر لحذف فيروس أتوران الموجود في القرص

goto :eof

open otmani.txt

هام جدا : هذه الطريقة مستعملة في البحث عن الفيروسات الرئيسية في الجهاز أما إذا كان هذا الفيروس دودة فيجب إتباع مخلفاته في الفلاش ديسك ومثال ذلك تجد ملفات وارد من نسختان وهي في الحقيقة ليست نسختان بل ملف صالح والملف الأخر فيروس يكون بصيغة ملف تطبيقي أو عند الدخول إلى مجلد تجده قد تم إعادته فقم بحذف الملف المعاد داخله مباشرة وهذه بعض حركات فيروس الدودة

انتهى والحمد لله

فنتمنى أن تستمتعوا مع هذه الطريقة وتكون مساهمة في رفع حماية الجهاز أكثر فلا تبخلونا بآرائكم

ملاحظة

إن التعديل في محتوى الكتاب يعرضك للمسألة أمام الله تعالى يوم القيامة

نرجو منك عدم التعديل في هذا الكتاب إلى بعلم صاحبه جزاكم الله خيرا

يمكنكم طرح مشاكلكم في مجال الفيروسات أو الحاسب على البريد التالي : cheriaala@yahoo.com

مع تحيات

مفكـــ بأفكار بلا حدود ـــر

الجزائـر